HDBOX

Heavy Duty Box - User Manual

Revision: July 30, 2015

Table of contents

INTRODUCTION 3

Driverless 3

Minimal Custom Cables 3

Dual Mode : Box / Clip mode 3

Keyboard Usage 4

Safe mode 4

Switching between box and clip modes 4

CHAPTER I - INSTALL, REGISTERING AND UPDATING 5

Installing 5

Registering 5

Firmware Update 5

Software Update 6

APP 8 - IPHONE USER CODE 7

Setting up a plan 7

Recommended plan 7

Running a plan 7

False positives 8

Advanced use - Quick Exit From Phone Disabled 8

Advanced use - Full keyboard support 8

Advanced use - Reading Infos ONLY 8

Clip mode use 9

APP 9 - EFI AND ICLOUD LOCK REMOVAL 10

Clip Mode 10

More about sync process 10

Mac Showing a Folder with exclamation mark on it 11

APP 6 - TFLASH DOCTOR 12

Under development 12

Introduction

HDBOX, or by its full name - Heavy Duty Box - it's a tool designed with GSM technician needs in mind and because of this it's having a nice list of features that will make every day use much more easy. Among this are the fact it is driverless, a minimal amount of cables are required to use it, can maintain the core of its functionality even without a computer and also have a safe mode to troubleshoot any possible issues.

Driverless

Being driverless means it can be moved from computer to computer with no problem, the only one driver actually required to use HDBox it is mass storage driver which is present on all computers and require almost no interaction from the user on the first install. Anything after it will be much more faster, with a cycle of max 2 seconds from the moment of connection to the moment the box can be used.

Minimal Custom Cables

At this moment, the only custom cable used by HDBox it's the light sensor cable required by the iPhone user code unlock process; and all other cables being used are standard cables available all through the industry and finding spares wont be an issue.

Dual Mode : Box / Clip mode

Ability of the tool to maintain its core functionality even without a computer it is a must have feature. In order to support this, HDBox, features full color display, a natural sounding speaker, and minimal set of physical buttons which does not require anything to activate them.

Box mode it is the most used and most complete mode when the box it is connected to pc and it is offering full control to the user. In this mode the user will be using management software available from website to control and can obtain a much more precise level of operation.

Clip mode it is the mode of use when the box it is not connected to a PC, and even without a computer HDBox still maintain it is core functionality.

Keyboard Usage

Two buttons are located on front panel: Cancel(X) and Confirm([]) and on righthand panel the selections switch its located, switch which provide triple functionality : up / down / select. The complete use of this buttons will be detailed for each applications, but basically use:

- **Cancel** will close the current app and return to neutral state, with no app running;
- **Confirm** will start / pause the activity of the app,
- **Up**/**Down** will adjust starting code,
- **Enter** will allow you to cycle between each parameters for the app and use up /down to modify them according to your need

Safe mode

In addition to the two normal operating modes HDBox features a third operating mode, safe mode, which can be trigged only on reset by holding down confirm button. In this mode box only loads an minimal set of drivers and this mode it is necessary only in extreme cases, and to exit from it users must either perform an update of the firmware or restart HDBox.

Switching between box and clip modes

If you need to switch modes this can be at start or restart of HDBox , or during normal operation.

To switch modes on box start simply press any button of the up / down / enter / escape while box its starting and it will start automatically in clip mode. Attention: if you press the confirm button during start, this will trigger safe mode.

During normal operation to switch from box mode to clip mode simply close current running APP and on main screen when it say “Press and hold enter for clip mode” , press and hold Enter for 2 seconds until green process bar will progress all the way to the right and clip mode will be launched.

To enter box mode from clip mode, simply exit current running app and navigate back to main menu, and using up/down navigate to the option “Goto Box mode” and selecting it to launch box mode.

Chapter I - Install, Registering and Updating

Installing

After connecting HDBox to PC for the first time, Windows will begin the process of installing the drivers for the box, process which might take up to a few minutes. After this initial process it's completed any sub-sequential connections will be much more faster.

NOTE: In the eventuality that windows does not seems to react to box connection and it is not installing the drivers, please check that the box its not in clip mode - HDBox it's showing a menu on screen and there is an "Goto Box Mode" option in it. In this case simply select that option and box will connect to PC.

Registering

To perform updates of the firmware there is no need to register, but it in order to access certain functionality the tool must be bound to a user account, bounding which can be done only during registration.

~~In order to register open management software and select about tab. First panel will display information about HDBox and if its register or not. If it is showing User: NOT REGISTERED, then the box can be registered to your account. To register it, simply click register button and fill up username, password, and optional reseller name and date of purchase. If you choose register as new user, the user will be first created and only after user was created successfully the box will be bound this user, but if you add it to an already existing account, the software will check on server the username and password, and only after the check pass, the box will be added to this user account.~~

Firmware Update

In same tab, user can manage the software running on the HDBox and update the box operating bios and manage the apps installed on it. Please do note, that it is strongly recommended to close any running apps before attempting performing any updates. In case that the bios / operating system received an upgrade the box will restart itself after 3 seconds in order to apply this updates.

Software Update

Last panel in about tab its software update panel. Here you can see the local version of your management software and swell the latest version available from our server. When clicking update button, the manager will download the new version and after the download its complete, a full scan of the download will be performed to ensure that the update was indeed done properly and the whole information was received. After all checks are passed the current running version of HDBox manager will close and the new version will be launched shortly.

Applications - Or in short apps, after packages that can be installed / modified independently and once launched they will take over the interface of HDBox and user can use interact directly with them. Apps available at this moment are **APP8 - iPhone user code**, **APP9 - EFI & iCloud lock removal** and **APP 6 - TFlash Doctor**. Upcoming chapters will detailed each one of them and how to use them.

APP 8 - iPhone user code

This app was developed to help recovering forgotten user codes on iPhone and iPads running IOS6, IOS7, IOS8.0 and IOS 8.1, and also features options that can work on even newer versions of IOS. To perform this process the light sensor it is required, and after the light sensor and an iPhone / iPad are connected to box the process can be started.

Setting up a plan

In order to unlock an iPhone a brute force attack must be performed, and to do this you will need a plan. Each plan must contain at least one step, and each step will be executed one by one from top to bottom. Each step can contain any number of codes, any codes that were already tested in previous steps will be skipped and there is no worry or need to remove overlapping codes from different steps. Codes will be remembered even on different plans or runs as long the same phone its connected or user did not reset the tried codes.

Recommended plan

We recommend this plan that will be testing all codes 0000 - 9999 and catch any most used codes at early stages, saving a lot of time on the long run

- Step1 — Consecutive Digits (Asc) — contains 0123, 1234, 2345, 3456, 4567, 5678, 6789, 7890, 8901, 9012
- Step2 — Consecutive Digits (Des) — contains 3210, 4321, 5432, 6543, 7654, 8765, 9876, 0987, 1098, 2109
- Step3 — Snake Combo — contains all possible combinations by moving left / right / up / down on keypad. Examples: 1258, 6980, 4565.
- Step4 — 0000 - 9999 — will test all numbers from 0000 to 9999 and because our tool remembers already tried codes, will only test the codes that weren't tested by previous steps.

Running a plan

After you setup the plan and carefully placed the light sensor on the corner of the display, you are ready to run the plan by pressing “RUN”. The plan will stop when the

difference on light its over the threshold or all codes were tested. If you need to stop the plan, you can press cancel, and after additional tweaks to it, click run again. Plan will run again, and any already tested codes will be skipped. If you need to start fresh and test all codes over again, simply press “xxx codes tried. Click to reset” and all previous tested codes will be forgotten and will be tested again in the step that contain them.

False positives

Because the detection of the good code it is based on changes of level of brightness of the phone display there is a chance to have false positives, and to continue the process after a false positive, simply click run button again, and the process will resume from last tried code, skipping all previous tested codes.

Advanced use - Quick Exit From Phone Disabled

In case that you know the user code but iPhone it is disabled you can use the single code enter functionality to quickly get iPhone out of disabled state. Just type the code and click “Send code” and phone should come out of disabled state. This option can support alfa-numeric codes as well, and works only IOS7.x and earlier versions of IOS.

Advanced use - Full keyboard support

In “Send code” interface a full keyboard its implemented and user can use it to send special characters to iPhone, by simply typing them and press send. Apart from normal letters and digits all possible symbols present on a normal full keyboard are implemented.

Advanced use - Reading Infos ONLY

If you just want read the info of the phone, then the light sensor cable it is not required and you only need to connect the iPhone to the box. A full list of info will be displayed , this list containing: IOS version, what model /size / color is the phone, when it was made, for what area it was made, phone family model as well. Anytime you connect a new iPhone, the informations will be read automatically and displayed on the screen.

Clip mode use

In order to lunch this APP in clip mode, you must bring your tool in clip mode and select this app from the list of installed apps and run it.

To enter clip mode simply press enter key (enter key = press the select switch located on righthand panel) and hold it until green bar progress all they way to the right. Total time its 2 seconds and it was implemented to prevent any accidental activations of clip mode.

From the menu displayed simply navigate up / down using the select switch up / down functionality and highlight desired app and press enter to run the app.

Once the app it is running you press confirm to start the process , or can use enter to start editing parameters like starting code, mode, and when everything its setup press confirm button to start the process.

If you need to pause the process to adjust light sensor position or anything else, simply press confirm while the process it is running, and process will pause, and after the adjustments of the light sensor, press confirm to resume the process.

False positives - In case of false positives simple press confirm button and the box will continue the process from last code entered.

Considering this process can take more than a couple of hours you might need to move the box or simply shut it down and resume the next day, we have implemented autosave functionality every 25 codes (we autosave each 25 codes and not each 1 because flash of our box have a limited number of rewrites, and even with our spread-write algorithm the technical limit of write cycles will be reached in about 1 year of permanent use if we had indeed autosaved each code. But with auto save each 25 codes the technical limit will be reached in 25 years, period what we think will satisfy everyone)

If you want to force an autosave simple press confirm to pause the process, then press confirm again to resume the process. The state of the process its autosaved on each start/ resume.

Box can remember for last and 5 more connected iPhones the process state and user code, so even if you run out of power, or simply disconnect / reset the box you only lose at maximum 25 codes which it is about 5minutes of work time. This informations are saved together in what we call sessions.

Sessions list it is visible from manager software, iPhone app tab, where you have full control over like, like add, modify, delete.

APP 9 - EFI and iCloud lock removal

This app was developed to help finding EFI code and in removal of iCloud lock. EFI lock appears when you try to boot your mac from other location than main drive and might be required if you plan on doing a clean install of OS. iCloud lock appears when a device its bound to a user iCloud account and the user activates the lock on it. This is a common problem when purchasing a second hand mac and original owner want to force the new owner to pay more than the price they agreed upon.

Because this app must take over the Usb Connection to the PC, it is not available to use from within manger software and can be used only from clip mode.

Clip Mode

When you start the app the default mode will be EFI and starting from code 0000 in ascending mode. To switch between EFI and iCloud mode simply press enter till you reach EFI / iCloud field and use up / down to switch between modes. Please note that for iCloud mode there its 2 additional steps that can be configured: “Waiting x minutes” and “Out of x minutes”. This options are required because iCloud process got dynamic timers and waiting time it is not constant.

When using it in EFI mode, the box will enter a code each 5 seconds, and total estimated time to try all possible codes it is about 16 Hours 45 minutes, and for iCloud the total maximum estimated time it is about 21 days and half.

When the code was found the progress bar will go green, and remain like that until user either exit the app or start another process.

During iCloud lock removal process there is no risk of false positives and the light sensor it is not required as well. The only possible issue can be that when the process was started the user did not sync properly the box to the mac timers, so to ensure that the sync process was done correct we recommend that the box will be monitored until first 1 minute waiting period and if both box and mac display same timer, and when the 1 minute timer expire box will enter the code in 5 seconds, then all it is good and can be left to run on its own.

More about sync process

Because waiting timers during iCloud lock removal process varies between instant, 1 minute, 5 minutes, 15 minutes, it is very IMPORTANT that user select the right “waiting xx minutes” and “Out of xx minutes”. If you are unsure about how long was the original waiting period, simply wait for it , then enter a code by hand, and you will see the new waiting period, and select on box “Waiting X minutes” na d”Out of X minutes” where x its number of minutes displayed on screen.

Mac Showing a Folder with exclamation mark on it

In the case your mac it is showing a folder icon with exclamation mark on it means that it cannot find its operation system, but a quick fix for most of the times it is when you reboot, press and hold command + R will take you to system utility where an EFI password might be required. After one more reboot mac might resume normal operations or take you to iCloud lock screen.

APP 6 - TFlash Doctor

Under development

This app it is development at this moment, and full list of features will be released near launch day.

This app was developed to enable users with full control and direct raw access to tFlash cards. Users can use this application to easily read the CID / CSD registers of the card, perform quick tests to verify that the card it is indeed the reported size, test card speed class, and gain direct - raw access to card sectors.